SCIENTIFIC CONFERENCE OPEN PROCEEDINGS
Global Academic Knowledge Repository

KIBERJINOYATLARNING TURLARI VA ULARGA QARSHI KURASHISHNI TAKOMILLASHTIRISH MASALALARI

Isroilov Odiljon Oqiljonovich
O‘zbekiston Respublikasi Ichki ishlar vazirligi akademiyasi kursanti

https://doi.org/10.5281/zenodo.23496224

Annotatsiya: Ushbu ilmiy maqolada zamonaviy axborot-kommunikatsiya texnologiyalari, raqamli infratuzilma va internet tarmog‘ining jadal rivojlanishi sharoitida kiberjinoyatlarning nazariy-huquqiy tabiati, ularning kriminologik mohiyati hamda asosiy turlari tasnifi tahlil qilingan. Kiberjinoyatchilikka qarshi kurashishning xalqaro standartlari, milliy jinoiy qonunchilikdagi normalar tizimi hamda kiberfazodagi xavf-xatarlarning o‘ziga xos xususiyatlari ochib berilgan.

Kalit so‘zlar: kiberjinoyat, axborot texnologiyalari, kiberxavfsizlik, raqamli makon, fishing, fishing, zararli dastur, kiberhujum, jinoiy javobgarlik, kriminologik tasnif.

XXI asr axborot jamiyati va global raqamlashtirish davrida iqtisodiyot, davlat boshqaruvi, bank-moliya sektori hamda fuqarolarning kundalik hayoti axborot texnologiyalari bilan uzviy bog‘landi. Biroq raqamli transformatsiyaning keng ko‘lamda kechishi, sun’iy intellekt, bulutli texnologiyalar va virtual to‘lov tizimlarining rivojlanishi bir vaqtning o‘zida kiberjinoyatchilik deb ataluvchi global va murakkab tahdidning jadallashuviga turtki bo‘ldi [1].

Kiberjinoyatlar an’anaviy jinoyatchilik shakllaridan o‘zining transchegaraviyligi, yuqori darajadagi maxfiyligi (anonimligi), iz qoldirish mexanizmlarining o‘zgaruvchanligi hamda yetkaziladigan moddiy va ma’naviy zararning keng qamrovliligi bilan keskin farq qiladi [2]. Bugungi kunda kompyuter tizimlariga noqonuniy kirish, bank kartalaridagi mablag‘larni talon-toroj qilish, shaxsga doir ma’lumotlarni o‘g‘irlash va strategik infratuzilma obyektlariga kiberhujumlar uyushtirish davlatlarning milliy va iqtisodiy xavfsizligiga bevosita xavf tug‘dirmoqda. Shu bois, kiberjinoyatlarning turlari, ularning yuzaga kelish shart-sharoitlari hamda ularga qarshi kurashish tizimini takomillashtirish masalalarini chuqur ilmiy-nazariy tahlil qilish dolzarb ahamiyat kasb etadi.

Yuridik adabiyotlar va kriminologiya fanida kiberjinoyat tushunchasiga turlicha yondashuvlar mavjud. Keng ma’noda, kiberjinoyat — kompyuter texnikasi, axborot tizimlari yoki telekommunikatsiya tarmoqlaridan jinoyat sodir etish quroli, vositasi yoki bevosita jinoyat obyekti (nishoni) sifatida foydalaniladigan qasddan sodir etilgan ijtimoiy xavfli qilmishlar majmuidir [3].

O‘zbekiston Respublikasining 2022-yil 15-apreldagi «Kiberxavfsizlik to‘g‘risida»gi O‘RQ-764-son Qonuniga muvofiq, kiberxavfsizlik kiberfazoda shaxs, jamiyat va davlat manfaatlarining tashqi va ichki tahdidlardan himoyalanganlik holati sifatida belgilanadi [4]. Ushbu qonuniy me’yor kiberjinoyatchilikka qarshi

faoliyat faqatgina huquq-tartibot organlarining jazo choralaridan iborat bo‘lmasdan, balki keng qamrovli texnologik, tashkiliy va profilaktik himoyani talab qilishini anglatadi.

Xalqaro tajriba, xususan, Budapesht konvensiyasi (2001) standartlari hamda O‘zbekiston Respublikasi Jinoyat kodeksi normalariga tayangan holda kiberjinoyatlarni quyidagi asosiy guruhlarga tasniflash mumkin [5]:

1. Axborot tizimlari va ma’lumotlar daxlsizligiga qarshi jinoyatlar:

Kompyuter axborotiga qonunga xilof ravishda (ruxsatsiz) kirish (JK 278¹-modda): himoyalangan tizimlarga xakerlik hujumlari, parollarni buzish yoki zaifliklardan foydalangan holda axborotni egallash;

Kompyuter axborotini modifikatsiyalash, yo‘q qilish yoki bloklash (JK 278²-modda);

Zararli dasturlarni (viruslar, troyanlar, ransomware-tovlamachi dasturlar) yaratish, ishlatish va tarqatish (JK 278⁴-modda).

2. Axborot texnologiyalari vositasida sodir etiladigan mulkiy jinoyatlar (kiberfiribgarlik):

Fishing va ijtimoiy injiniring: soxta veb-sahifalar, havolalar yoki qo‘ng‘iroqlar orqali fuqarolarning bank kartasi ma’lumotlari va maxfiy SMS-kodlarini aldov yo‘li bilan qo‘lga kiritish;

Kriptovalyuta va virtual aktivlar bilan bog‘liq firibgarliklar: moliyaviy piramidalar, soxta birjalar va tokenlar vositasida mablag‘larni noqonuniy o‘zlashtirish [6].

3. Infratuzilma va servislar faoliyatiga qarshi tajovuzlar:

DDoS (Distributed Denial of Service) hujumlari: serverlar va axborot resurslariga sun’iy so‘rovlar oqimini yuborish orqali ularning ish faoliyatini to‘xtatib qo‘yish.

4. Kiberfazodagi shaxsiy daxlsizlik va jamoat xavfsizligiga qarshi jinoyatlar:

Kibertahdid, kiberbulling, shantaj (doksing) hamda ekstremistik, radikal yoki pornografik materiallarni internet orqali qonunga xilof ravishda tarqatish [7].

Mazkur tasnif kiberjinoyatchilikning ko‘p vektorli va dinamik ekanligini ko‘rsatadi. Ushbu qilmishlarga qarshi samarali kurashish ularning huquqiy kvalifikatsiyasini to‘g‘ri amalga oshirish hamda fosh etish mexanizmlarini zamonaviylashtirishni talab etadi.

O‘zbekiston Respublikasida ichki ishlar organlari va boshqa huquqni muhofaza qiluvchi idoralar tomonidan kiberjinoyatlarga qarshi kurashish borasida amalga oshirilayotgan tezkor-qidiruv va tergov amaliyoti tahlil qilinganda, texnik ta’minot va mutaxassislar malakasini oshirish choralari ko‘rilayotganiga qaramasdan, sohada bir qator tizimli to‘siqlar saqlanib qolayotganini ko‘rish mumkin. O‘zbekiston Respublikasi Prezidentining 2021-yil 29-noyabrdagi PF-27-son «O‘zbekiston Respublikasi jamoat xavfsizligi konsepsiyasini tasdiqlash to‘g‘risida»gi Farmonida kiberfazoda xavfsizlikni ta’minlash va kiberjinoyatlarni barvaqt fosh etish ustuvor yo‘nalishlardan biri sifatida belgilangan [8].

Biroq amaliyotda kiberjinoyatlarning oldini olish va ularni tergov qilish jarayonida quyidagi tizimli muammolar ko‘zga tashlanmoqda:

1. Kiberjinoyatchilarning yuqori darajadagi anonimligi va texnik vositalardan foydalanishi

Zamonaviy kiberjinoyatchilar o‘z shaxsini yashirish maqsadida ko‘p bosqichli himoya vositalaridan keng foydalanadilar:

Proksi-serverlar, VPN (Virtual Private Network) va Tor tarmoqlari: Haqiqiy IP-manzilni bir necha xorijiy davlatlar serverlari orqali yashirish orqali tergov organlarining raqamli izlarni tezkor topishiga to‘sqinlik qilinadi;

«Drop» (dropper)lar tarmog‘i va sim-kartalarni noqonuniy rasmiylashtirish: Kiberfiribgarlar o‘g‘irlangan mablag‘larni uchinchi shaxslar (talabalar, ishsiz fuqarolar) nomiga ochilgan bank kartalari orqali zanjirli ravishda o‘tkazib, keyinchalik kriptovalyutaga aylantiradilar yoki naqdlashtiradilar. Natijada jinoyatning haqiqiy tashkilotchilarini aniqlash jarayoni o‘ta murakkablashadi [9].

2. Raqamli (elektron) dalillar bilan ishlashdagi protsessual qiyinchiliklar

Kiberjinoyatlarni tergov qilishda an’anaviy kriminalistik usullar ko‘pincha yetarli samara bermaydi. Jinoyat-protsessual qonunchiligida quyidagi amaliy bo‘shliqlar mavjud:

Raqamli ma’lumotlarning dinamikligi va tez o‘chib ketishi: Server loglari, tarmoq trafigi va ma’lumotlar almashinuvi bir necha soat yoki kun ichida yangilanadi yoki o‘chiriladi. Amaldagi JPK bo‘yicha tergovchining so‘rovi yoki sud ajrimini olish uchun talab etiladigan protsessual vaqt sababli muhim dalillar yo‘qotilishi xavfi yuqori bo‘lib qolmoqda [10];

Elektron dalillarning daxlsizligi zanjiri (Chain of Custody): Voqea joyidan kompyuter texnikasi, mobil qurilmalar va serverlarni olib qo‘yishda ularning xesh-summasini hisoblash, ma’lumotlarning o‘zgarmasligini kafolatlash bo‘yicha tergovchilarda ixtisoslashgan texnik ko‘nikmalar va yagona standartlashtirilgan protsessual qo‘llanmalar yetishmaydi.

3. Xalqaro tezkor hamkorlikning sekinligi va yurisdiksiya chegaralari

Kiberjinoyatlarning transchegaraviy xarakteri sababli jinoyatchi bir davlatda, jabrlanuvchi ikkinchi davlatda, jinoyat sodir etilgan serverlar esa uchinchi davlatda joylashgan bo‘ladi.

An’anaviy xalqaro huquqiy yordam ko‘rsatish kanallari (diplomatik yo‘llar, Bosh prokuratura orqali yuboriladigan xatlar) orqali ma’lumot olish oylar davom etadi. Kiberfazoda esa bunday kechikish jinoyat izlarining butunlay yo‘q qilinishiga olib keladi [11];

Ommabop xorijiy messenjerlar (Telegram, WhatsApp) va ijtimoiy tarmoqlar (Meta, Google) ma’muriyati bilan tezkor, to‘g‘ridan-to‘g‘ri hamkorlik mexanizmlarining to‘liq yo‘lga qo‘yilmaganligi axborot olish jarayonini qiyinlashtiradi.

4. Aholining raqamli va moliyaviy savodxonligi darajasining pastligi (Viktimologik omil)

Kiberjinoyatlarning, xususan, kiberfiribgarliklarning o‘sishiga fuqarolarning axborot xavfsizligi qoidalariga rioya qilmasligi bevosita zamin yaratmoqda. Ko‘plab fuqarolar firibgarlarning psixologik bosimi va aldoviga uchrab, o‘zlarining maxfiy SMS-kodlarini, bank kartasi parollarini o‘z qo‘llari bilan begonalarga berib qo‘ymoqdalar [12].

Ushbu amaliy muammolar kiberjinoyatlarga qarshi kurashishda qonunchilikni modernizatsiya qilish, tergov organlarining kiberforensika imkoniyatlarini kuchaytirish hamda keng qamrovli profilaktik chora-tadbirlarni amalga oshirish zarurligini yaqqol ko‘rsatadi.

Kiberjinoyatchilikning transchegaraviy va dinamik xarakteri mazkur sohadagi kurashni faqat an’anaviy tergov usullari bilan cheklab bo‘lmasligini ko‘rsatadi. Ushbu xavf-xatarlarni barvaqt jilovlash, raqamli dalillar bilan ishlash mexanizmlarini zamonaviylashtirish va amaliyot samaradorligini oshirish maqsadida quyidagi ilmiy-amaliy taklif va tavsiyalar ilgari suriladi:

Ilmiy-amaliy taklif va tavsiyalar

1. Jinoyat-protsessual qonunchiligida «Raqamli (elektron) dalillar» institutini takomillashtirish.
   O‘zbekiston Respublikasi Jinoyat-protsessual kodeksiga elektron dalillarni aniqlash, ko‘zdan kechirish, olib qo‘yish va ularning yaxlitligini ta’minlash (Chain of custody) tartibini belgilovchi maxsus normalarni kiritish lozim. Shuningdek, telekommunikatsiya operatorlari va internet-provayderlar bazasidagi dinamik ma’lumotlarni (server loglari, tarmoq trafigi) tergovchining asoslantirilgan qarori bilan sud qarorigacha bo‘lgan davrda shoshilinch muzlatib qo‘yish (Expedited preservation) mexanizmini joriy etish zarur [13].
2. «Drop»-kartalar aylanmasiga qarshi jinoiy javobgarlikni kuchaytirish.
   O‘zbekiston Respublikasi Jinoyat kodeksiga bank kartalari, elektron hamyonlar va ularga bog‘langan hisob raqamlarini uchinchi shaxslarga noqonuniy ravishda moddiy manfaat evaziga berish («drop» faoliyati) yoki ularni kiberjinoyatdan tushgan mablag‘larni naqdlashtirish uchun yig‘ish harakatlarini mustaqil jinoyat tarkibi sifatida kiritish tavsiya etiladi.
3. Banklar, to‘lov tashkilotlari va IIV o‘rtasida «Antifrod» (Anti-fraud) tezkor integratsiyasini yo‘lga qo‘yish.
   Shubhali moliyaviy operatsiyalarni real vaqt rejimida to‘xtatish imkonini beruvchi yagona avtomatlashtirilgan axborot tizimini ishga tushirish zarur. Agar firibgarlik yo‘li bilan pul o‘tkazilganligi to‘g‘risida xabar kelib tushsa, mablag‘ keyingi zanjirlarga chiqib ketmasligi uchun tergov organlari va

banklar o‘rtasidagi tezkor elektron buyruq orqali hisob raqamni bir necha daqiqa ichida avtomatik bloklash mexanizmi yaratilishi shart [14].

4. Kiberforensika laboratoriyalarini xalqaro standartlar (ISO/IEC 27037) asosida rivojlantirish.
   Ichki ishlar organlari va sud-ekspertiza markazlarining raqamli kriminalistika bo‘linmalarini zamonaviy apparat-dasturiy komplekslar bilan ta’minlash, ekspert va tergovchilarning kiberxavfsizlik, xakerlik izlarini tahlil qilish hamda kriptovalyutalar tranzaksiyalarini kuzatish (blockchain-analytics) bo‘yicha ixtisoslashgan malakasini tizimli oshirish lozim.
5. Aholining kibergigiyena va moliyaviy savodxonligini oshirish bo‘yicha doimiy viktimologik profilaktika.
   Aholining barcha qatlamlarini, ayniqsa keksalar va yoshlarni qamrab oluvchi «Kiberxavfsiz jamiyat» ommaviy axborot kampaniyasini kengaytirish, firibgarlikning yangi sxemalari (fishing, soxta qo‘ng‘iroqlar, soxta investitsiya loyihalari) haqida SMS-ogohlantirishlar va OAV orqali muntazam profilaktik tushuntirish ishlarini olib borish lozim [15].

Xulosa qilib aytganda, kiberjinoyatchilik an’anaviy kriminologik qoliplarni butunlay o‘zgartirib, milliy xavfsizlik va iqtisodiy barqarorlikka bevosita tahdid soluvchi global muammoga aylandi. Ushbu qilmishlarga qarshi faqatgina jabrlanuvchi murojaat qilgandan keyingi javob choralari bilan kurashish samarasizdir.

Kiberjinoyatlarga qarshi kurash tizimini takomillashtirish qonunchilik bazasini zamonaviy tahdidlarga moslashtirish, tezkor-qidiruv va tergov amaliyotini ilg‘or kiberforensika texnologiyalari bilan qurollantirish, bank tizimi bilan tezkor bloklash mexanizmlarini integratsiya qilish hamda aholining raqamli madaniyatini oshirish orqali kompleks yondashuvni taqozo etadi. Faqat texnologik va huquqiy jihatdan mukammal himoyalangan kiberfazo fuqarolarning daxlsizligi hamda mamlakat raqamli iqtisodiyotining ishonchli rivojlanishini kafolatlaydi.

REFERENCES:

1. O‘zbekiston Respublikasining «Kiberxavfsizlik to‘g‘risida»gi Qonuni. O‘RQ-764-son. 15.04.2022-y. // Qonunchilik ma’lumotlari milliy bazasi (lex.uz).
2. Maras M.H. Cybercriminology. – Oxford: Oxford University Press, 2016. – 416 p.
3. Rustamboyev M.H. O‘zbekiston Respublikasi Jinoyat huquqi kursi. Maxsus qism. 4-tom: Iqtisodiyot sohasidagi jinoyatlar. Axborot texnologiyalari sohasidagi jinoyatlar. – Toshkent: TDYU nashriyoti, 2018. – 396 b.

4. O‘zbekiston Respublikasining Jinoyat kodeksi. Rasmiy nashr. – Toshkent: Adolat, 2023. – 480 b.
5. Council of Europe. Convention on Cybercrime (ETS No. 185). Budapest, 23.XI.2001. – Strasbourg: Council of Europe, 2001. – 28 p.
6. Clough J. Principles of Cybercrime. 2nd ed. – Cambridge: Cambridge University Press, 2015. – 464 p.
7. Юлдашев, Д. Х. (2025). ИЧКИ ИШЛАР ОРГАНЛАРИ ХОДИМИНИНГ ИМИЖИНИ ЯХШИЛАШГА ДОИР ЗАМОНАВИЙ ЁНДАШУВЛАР. Central Asian Journal of Education and Innovation, 4(8), 93-97.
8. O‘zbekiston Respublikasi Prezidentining 2021-yil 29-noyabrdagi PF-27-son «O‘zbekiston Respublikasi jamoat xavfsizligi konsepsiyasini tasdiqlash to‘g‘risida»gi Farmoni // Qonunchilik ma’lumotlari milliy bazasi (lex.uz).
9. Brenner S.W. Cybercrime: Criminal Threats from Cyberspace. – Santa Barbara: Praeger, 2010. – 281 p.
10. O‘zbekiston Respublikasining Jinoyat-protsessual kodeksi. Rasmiy nashr. – Toshkent: Adolat, 2023. – 568 b.
11. Xayitovich, Y. J. (2021). Admission to the citizenship of the Republic of Uzbekistan in a simplified manner basics and conditions. ACADEMICIA: An International Multidisciplinary Research Journal, 11(3), 1421-1424.
12. Karimova V.M. Ijtimoiy psixologiya: Darslik. – Toshkent: O‘zbekiston faylasuflari milliy jamiyati, 2012. – 240 b.
13. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 3rd ed. – London: Academic Press, 2011. – 840 p.
14. Xayitovich, Y. D. (2026). TRANSPORT HUQUQI MUSTAQIL HUQUQ TARMOQI SIFATIDA: NAZARIY ASOSLAR, QIYOSIY TAHLIL VA O‘ZBEKISTON QONUNCHILIGINI TAKOMILLASHTIRISH MASALALARI. Eurasian Journal of Law, Finance and Applied Sciences, 6(2), 67-71.
15. Boboyev H.B. Huquqiy madaniyat va kasbiy odob-axloq qoidalari: O‘quv qo‘llanma. – Toshkent: Adolat, 2017. – 192 b.